PCT COOPERATION TREATY

PCT

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

(PCT Article 36 and Rule 70)

Applicant's or agent's file reference STSWO54	**FOR FURTHER ACTION**	See Notification of Transmittal of International Preliminary Examination Report (Form PCT/IPEA/416)
International application No. PCT/US03/02931	International filing date *(day/month/year)* 30 January 2003 (30.01.2003)	Priority date *(day/month/year)* 30 January 2002 (30.01.2002)
International Patent Classification (IPC) or national classification and IPC IPC(7): H04L 9/32 and US Cl.: 713/186		
Applicant TECSEC, INC.		

1. This international preliminary examination report has been prepared by this International Preliminary Examining Authority and is transmitted to the applicant according to Article 36.

2. This REPORT consists of a total of 6 sheets, including this cover sheet.

   ☐ This report is also accompanied by ANNEXES, i.e., sheets of the description, claims and/or drawings which have been amended and are the basis for this report and/or sheets containing rectifications made before this Authority (see Rule 70.16 and Section 607 of the Administrative Instructions under the PCT).

   These annexes consist of a total of — sheets.

3. This report contains indications relating to the following items:

   - I ☒ Basis of the report
   - II ☐ Priority
   - III ☐ Non-establishment of report with regard to novelty, inventive step and industrial applicability
   - IV ☐ Lack of unity of invention
   - V ☒ Reasoned statement under Article 35(2) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement
   - VI ☐ Certain documents cited
   - VII ☐ Certain defects in the international application
   - VIII ☐ Certain observations on the international application

Date of submission of the demand	Date of completion of this report
29 August 2003 (29.08.2003)	05 January 2004 (05.01.2004)
Name and mailing address of the IPEA/US Mail Stop PCT, Attn: IPEA/US Commissioner for Patents P.O. Box 1450 Alexandria, Virginia 22313-1450 Facsimile No. (703) 305-3230	Authorized officer Ayaz Sheikh Telephone No. 703-305-9648

Form PCT/IPEA/409 (cover sheet)(July 1998)

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/US03/02931

I. Basis of the report

1. With regard to the elements of the international application:*

☒ the international application as originally filed.

☒ the description:
pages 1-75 as originally filed
pages NONE, filed with the demand
pages NONE, filed with the letter of _____.

☒ the claims:
pages 76-93, as originally filed
pages NONE, as amended (together with any statement) under Article 19
pages NONE, filed with the demand
pages NONE, filed with the letter of _____.

☒ the drawings:
pages 1-22, as originally filed
pages NONE, filed with the demand
pages NONE, filed with the letter of _____.

☐ the sequence listing part of the description:
pages NONE, as originally filed
pages NONE, filed with the demand
pages NONE, filed with the letter of _____.

2. With regard to the **language**, all the elements marked above were available or furnished to this Authority in the language in which the international application was filed, unless otherwise indicated under this item.
These elements were available or furnished to this Authority in the following language _____ which is:

☐ the language of a translation furnished for the purposes of international search (under Rule23.1(b)).

☐ the language of publication of the international application (under Rule 48.3(b)).

☐ the language of the translation furnished for the purposes of international preliminary examination(under Rules 55.2 and/or 55.3).

3. With regard to any **nucleotide and/or amino acid sequence** disclosed in the international application, the international preliminary examination was carried out on the basis of the sequence listing:

☐ contained in the international application in printed form.

☐ filed together with the international application in computer readable form.

☐ furnished subsequently to this Authority in written form.

☐ furnished subsequently to this Authority in computer readable form.

☐ The statement that the subsequently furnished written sequence listing does not go beyond the disclosure in the international application as filed has been furnished.

☐ The statement that the information recorded in computer readable form is identical to the written sequence listing has been furnished.

4. ☒ The amendments have resulted in the cancellation of:

☒ the description, pages NONE

☒ the claims, Nos. NONE

☒ the drawings, sheets/~~fig~~ NONE

5. ☐ This report has been established as if (some of) the amendments had not been made, since they have been considered to go beyond the disclosure as filed, as indicated in the Supplemental Box (Rule 70.2(c)).**

** Replacement sheets which have been furnished to the receiving Office in response to an invitation under Article 14 are referred to in this report as "originally filed" and are not annexed to this report since they do not contain amendments (Rules 70.16 and 70.17).*

*** Any replacement sheet containing such amendments must be referred to under item 1 and annexed to this report.*

INTERNATIONAL PRELIMINARY EXAMINATION REPORT

International application No.
PCT/US03/02931

V. Reasoned statement under Rule 66.2(a)(ii) with regard to novelty, inventive step or industrial applicability; citations and explanations supporting such statement

1. STATEMENT

Novelty (N)	Claims	7-30, 32-37, 39-58	YES
	Claims	1-6, 31, 38 AND 59	NO
Inventive Step (IS)	Claims	NONE	YES
	Claims	1-59	NO
Industrial Applicability (IA)	Claims	1-59	YES
	Claims	NONE	NO

2. CITATIONS AND EXPLANATIONS

Please See Continuation Sheet

Supplemental Box
(To be used when the space in any of the preceding boxes is not sufficient)

V. 2. Citations and Explanations:
Claims 1-6, 31, 38 and 59 lack novelty under PCT Article 33(2) as being anticipated by Gullman et al., US Pat. No. 5,280,527 issued Jan 1994.

Gullman teaches a biometric security mechanism which generates a security token which a user inputs to an access device. Gullman's security token is formed from biometric information (i.e. biometric-based data instance), a fixed code and, a time varying code, see col. 3, lines 37-55. Gullman's fixed code includes a PIN (i.e. knowledge-based data instance), embedded serial number, account number (i.e. possession-based data instance), see col. 2, lines 48-65.

Gullman further teaches that the security apparatus receives the biometric input, and then compares the biometric input to a stored template to derive a correlation factor. The correlation factor is combined with the fixed code to generate a security token (i.e. an authentication code).

Gullman further teaches that the security token is displayed on a display panel of the security apparatus where it is entered at an access code or is directly transmitted to a host system which decodes the token to identify the embedded fixed code and correlation factor, see col. 4, lines 3-22.

Gullman teaches that the host system determines whether to grant to user the access to the host system. This determination is based on a comparison made on a transmittable code which includes the above described authentication code, see col. 7, lines 1-33.

Claims 7-30 lack inventive step under PCT Article 33 (3) as being obvious over the prior art as applied in the immediately preceding paragraph and further in view of Gennaro et al, US Pat. No. 6,317,834 filed Jan. 1999.

As per claims 7, 9, 10 and 12-14, 25-26, Gullman teaches that the processor of the security apparatus may include a standard encryption module which applies an encryption algorithm to the time of day from real time clock, the fixed code (which includes PIN, serial number and account number) and a biometric correlation factor, generating an encrypted security token (that is, an encrypted authentication code). Gullman further teaches that the host system also includes a decryption module, capable of decrypting the encrypted code generated by the encryption module of biometric security apparatus, but fails to specifically disclose generating a key based on a first data instance of the plurality of factor-based data instances" and "interrogating the recovered data instance against the second data instance to generate an authentication value".

However, Gennaro teaches a method of performing biometric authentication of a person's identity including a biometric template prior to storing it in a biometric database, see abstract.

Gennaro's method further provides means for verifying the identity of an individual to authorize access to a general database comprising the steps of:

Acquiring a current biometric sample (i.e. a biometric-based data instance), acquiring a current personal identifier (i.e. a knowledge based data instance); acquiring decryption key generation data (i.e. a plurality of factor-based data instances); comparing the personal identifier with the database, and on a match with a personal identifier in the database; creating a decryption key from decryption key generation data; performing a decryption operation on the retrieved biometric (i.e. recovered biometric) record

Supplemental Box
(To be used when the space in any of the preceding boxes is not sufficient)

utilizing the decryption key to decrypt encrypted biometric model from the retrieved record. Comparing the decrypted biometric model with the current biometric sample to verify the individual as authorized to access the general database, see col. 2, line 6-21. see also Fig. 5 and 6.

Gennaro further teaches that a first encryption key is created from the user's password (i.e. one of factor of plurality of factor-base data instances) and is used to encrypt the biometric model. That is, a modified data instance is created based on a second data instance of a plurality of factor based data instances.

It would have been obvious to one ordinary skill in the art to modify Gullman's biometric security apparatus to employ Gennaro's method of authentication with encrypted models to store biometric information in a secure manner so as to prevent the occurrence of theft and attacks from unauthorized personnel, see also 1, lines 40-55.

As per claim 11, Gullman's encrypted security token includes an embedded serial number (i.e. a possession-based data instance), see col. 2, line 55-56.

As per claim 8, in another embodiment, Gennaro further teaches a key derived from a randomly chosen subset of answers obtained as a result of conducting a challenge question/answer session with the individual. Then, biometric template and the full set of answers are combined and encrypted. That is, the biometric record is comprised of the personal identifier and challenge list in plaintext, along with the encrypted answers (i.e. another authentication value) and biometric model (i.e. a first authentication value), see col. 9, lines 31-46, see also Fig. 7a.

As per claims 15-18 and 20-24, 27-30, Gullman teaches that the security apparatus initially is configured in an enroll mode where biometric samples or templates (i.e. first biometric data instance) are obtained. Gullman further teaches that the access device transmits a derived token (i.e. a second modified version of biometric data instance) to the host system, which decrypts or decodes the token to derive the fixed code and a correlation factor. If the fixed code identifies a valid user and the correlation factor is above the threshold level, then access is permitted, if not, then access is denied, see col. 6, lines 30-45.

Gullman fails to teach a modified version of first and second biometric data instance where the second modified version is a hash of second biometric-based data instance. However, use of hash function and message digest using a one directional hash function is well known in the art of cryptography, this is taken as official notice. It would have been obvious to one ordinary skill in the art to hash the biometric templates or samples of Gullman at enrollment for security and space requirement.

Claims 32-37, 39-58 lack inventive step under PCT Article 33(3) as being obvious over the prior art as applied in the immediately preceding paragraph and further in view of Boebert, US Pat. No. 5,499,297, issued Mar 1996 and further in view of Johnson et al, US Pat. No. 5,694,472, issued Dec. 1997.

Boebert is directed to a system and method for identifying and authentication users and for controlling the access of these users to privileged instructions within a data enclave, see abstract.

Boebert's invention uses a cryptography to protect the data on media and to distribute and protect the cryptographic keys in order to achieve security, flexibility, and ease of use.

Boebert's cryptographic services are used to prevent unauthorized access through the wide area network or the unauthorized use of privileged services, see col. 11, line 45 through col. 13, lines 57.

Boebert's protection of data (object) on media takes place in three broad phases: media initialization and key assignment to the individual user, requesting the initialization; assignment of a key for already initialized media to additional users; keying of devices, so access to the data may be made.

Boebert teaches that in media initialization and key generation phase a media key and an access vector for a unit of media is generated and placed in enciphered form in the personal keying device assigned to the individual requesting the initialization. This data is also stored in a security server to be restored at a later time. Boebert's access vector depends on user attributes as well as media attributes.

Boebert further teaches that in the keying of devices phase proper media key/access vector combination is automatically extracted from the personal keying device and are decrypted and used to allow controlled access to the unit of media.

Boebert discloses the media key/access vector combination are enciphered with a combination key (i.e. a working key) which includes the user's PIN, user's unique identifier (user UID), and an enclave key, see col. 13, lines 34-43.

Boebert teaches that when an already-initialized unit of media is to be shared with a user other than the one who initialized it, the individual desiring access to media enters his or her PIN into his personal keying device where the encrypted user UID is extracted and decrypted using the enclave key. Then, the Media UID is read and the personal keying device is searched for a Media key/Access vector for the unit of media or the user and a request packet consisting of the PIN, User UID, Media UID, encrypted using enclave key is sent to Security Server where the received packet is decrypted using the enclave key and stored the PIN, User UID, and request for later steps.

That is, Boebert's invention clearly suggest a user profile key encryption key and a profile associated with the user wherein the profile includes an enclave key (i.e. domain value) and an encrypted profile encryption key. Boeberts clearly suggest all elements of claim 1 using a symmetric key encryption.

To the extent that Boebert may not disclose the public key cryptography limitation in claim 1, a sufficient equivalent is disclosed by Johnson.

Johnson disclosed a personal access management system. The system provides for a user module to generate keys, which are combined with other keys (EKE). Public key techniques are taught at column 51, lines 1-53.

It would have been obvious to one ordinary skill in the art to modify Boebert's invention to that of Johnson's public key

Supplemental Box
(To be used when the space in any of the preceding boxes is not sufficient)

techniques to convey EKE for security reason, see Johnson's col. 23, lines 35-40.

Boebert teaches that at initialization the profile includes an access vector (i.e. profile and credential initialization vector), see col. 13, lines 34-43, see also, col. 3, lines 20-35.

Boebert invention clearly suggest an enclave key which is the same for all authorized users, that is multi-level access vector is identical to multi-level access identifier, see col. 9, lines 64-67.

Claims 1-59 meet industrial applicability as defined by PCT Article 33(4), because authentication may be used in various access control devices.

---------- NEW CITATIONS ----------